Link to Full Story

The (Secure) Digital Future of Healthcare

By Alex Nehmy, Regional Chief Security Officer – Critical Industries

Hospitals were first established to treat the sick around the fourth century CE (AD) and ever since, have been the place people attended when they were too unwell to stay in their homes. In early medieval Europe, it was believed that sickness was supernatural and therefore untreatable by humans. However, over the centuries, hospitals spread throughout the developed world and became places for the sick to gather and be treated.

Healthcare has, for over 1,000 years, been primarily focussed on treating the sick. It has essentially been sickness care. However, healthcare is undergoing the greatest revolution since the invention of the hospital—the digital revolution—and with this, we'll see a paradigm shift to that of wellness care.

The first digital medical devices began appearing in the healthcare setting in the 1960s and 1970s, and were mechanical devices with a few digital smarts. Digital infusion pumps, electrocardiogram machines, and CT scanners were some of the first medical devices to leverage digital capabilities.

Now, over 50 years later, the medical devices that are critical to providing positive health outcomes for patients are computer systems that perform highly complex and life-saving medical functions. Examples are digital ventilators, advanced pacemakers with implantable defibrillators, and robotic surgical systems.

Following the trajectory of the digitisation of medicine and the acceleration of telemedicine and remote healthcare that we saw during the pandemic, we're beginning to see, not only a digital future for healthcare, but also the future of remote medicine.

Smart medical devices will monitor your body around the clock, collecting valuable data and leveraging the smarts of AI to enable the early detection of health issues and provide timely intervention, helping keep you well and in your own home.

Healthcare professionals will have access to your health data and AI recommendations from a virtual hospital, anywhere in the world, where you'll receive care 24/7 on a schedule that suits you, rather than waiting for the doctor to do their rounds.

Smart medical devices, along with AI, will usher in an era of true wellness care, keeping people healthy and in their homes. Sickness care in a hospital will be reserved for only

the most unwell, freeing up hospital beds and easing the resource burden on the healthcare industry.

Much like shopping has changed from a physical location to a virtual experience, so too will healthcare. People will expect to stay in their homes, without the inconvenience of having to attend a hospital.

These smart medical devices won't only be indispensable in our digital health future, they'll also be ubiquitous. From smartwatches that continuously evaluate your heart health to digital contact lenses to monitor glucose levels, wearable healthcare devices will be everywhere. In fact, Apple CEO Tim Cook has said "Healthcare will be Apple's greatest contribution to mankind."

These smart medical devices are essentially computer systems. They run software, which must be accurate and consistent, to be relied upon to reliably monitor and treat patients. However, software has inherent weaknesses: it can be maliciously modified and often contains vulnerabilities.

A vulnerable medical device could be compromised by a threat actor and could be rendered unusable, preventing it from functioning at all, or it could be maliciously modified, causing it to malfunction. The result of a malfunctioning digital ventilator or an infusion pump delivering life-saving medication is likely to be fatal.

The closer a device is to a patient, the more likely it is to kill them. Gartner predicts that by 2025, an industrial device will be misused to harm or kill someone.[1]

Would you want your loved one in hospital, receiving life-saving treatment from a digital infusion pump that could malfunction at any moment?

The healthcare industry can focus on the following three approaches to ensuring the digital future is secure:

- Secure Build
  Device manufacturers must acknowledge the criticality of ensuring device integrity and build cybersecurity into every aspect of the device. From software to physically secure hardware, security must be considered and prioritised right from the design of the device to the final code. Smart medical devices must be built securely from the ground up.
- Secure Operation
  Upon deploying devices into the field, they must be configured securely to minimise the risk of compromise. Ensuring default passwords have been changed and hardening the configuration of the device is essential in ensuring its integrity.

  Additionally, healthcare institutions need to deploy these devices in secure network segments, with least-privileged access and protection from the latest threats.
- Secure Future
  Ongoing operation of these smart medical devices relies on vulnerabilities being identified and device software being kept up to date with regular patching schedules.

For healthcare to realise its digital future, it must build cybersecurity into everything it does and fiercely protect the integrity of these digital medical devices. Cybersecurity will be the fundamental enabler of healthcare's digital future.

1Reduce Risk to Human Life by Implementing This OT Security Control Framework, Gartner, June 17, 2021.